STATE OF ALABAMA

Information Technology Policy

Policy 640-03: Wireless Security

OBJECTIVE:
Establish the responsibilities for the secure deployment of wireless data and/or voice network capability onto State of Alabama network resources.

SCOPE:
This policy applies to all State of Alabama organizations that deploy wireless networks or devices, and covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of the State's internal networks.

RESPONSIBILITIES:
Access to State networks via unsecured wireless communication mechanisms is prohibited.

Wireless networks shall be centrally managed by the Information Services Division (ISD) of the Department of Finance for all organizations on the capitol campus served by ISD. Off-campus organizations may obtain their own wireless services after providing a security plan to the State IT Security Council for approval. All off-campus organizations shall register their wireless networks with ISD.

To ensure security and supportability, organizations shall procure only wireless products that meet State standards.

IT Managers and Network Administrators shall ensure that only wireless systems deployed in compliance with applicable State standards are approved for connectivity to State networks unless granted an exclusive waiver by the State CIO.

ENFORCEMENT:
Refer to Information Technology Policy 600-00: Information Security.

Signed by Jim Burns, Chief Information Officer

Policy History

Version	Release Date	Comments
Original	2/13/2007	